National Security Agency

Bridge Certification Authority Technology Demonstration

Briefing for Federal Public Key Infrastructure Technical Working Group
8 September 1999

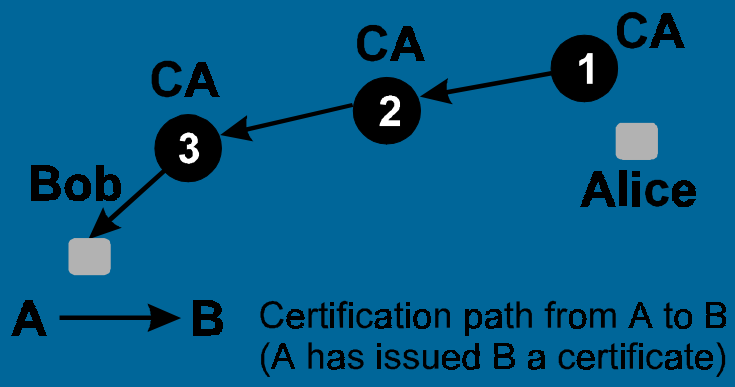
Dave Fillingham, NSA
dwfilli@missi.ncsc.mil
dwfilli@nsa

Overview

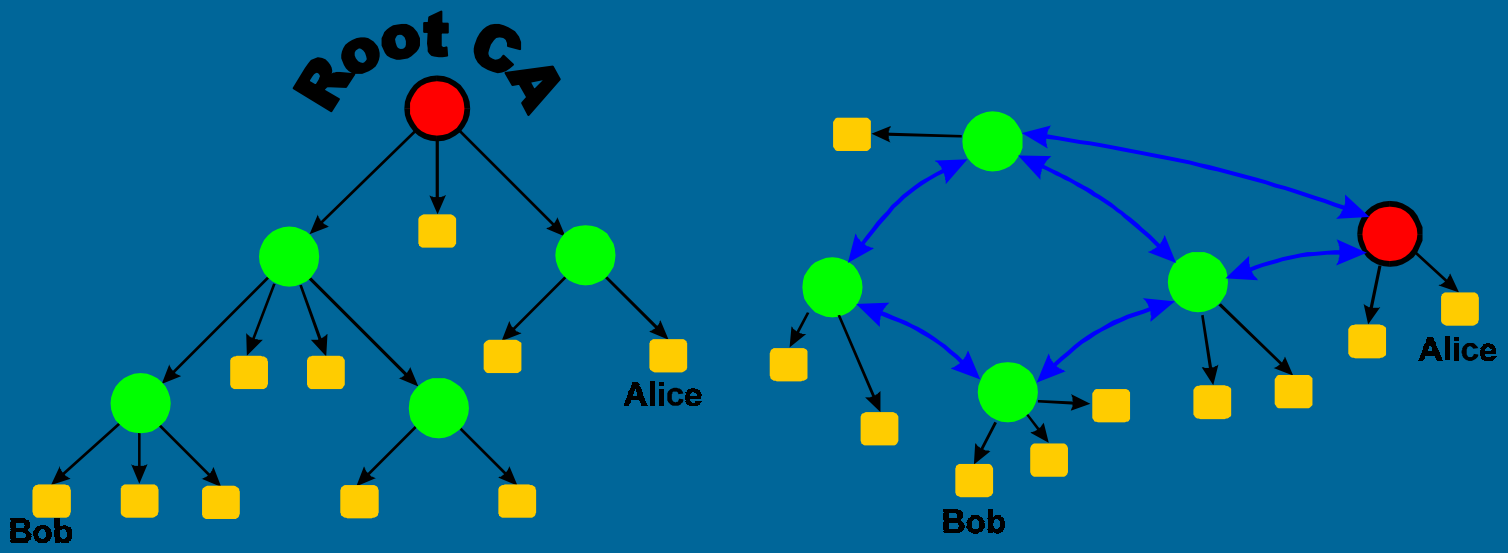
- Bridge CA Background
- Demonstration Purpose
- Participants
- Overall Architecture
- Status
- Products

Certification Path

- Alice can verify Bob's certificate by verifying a chain of certificates ending in one issued by a Certification Authority (CA) she trusts (and whose public key she knows)



PKI Structure



a. hierarchical infrastructure

b. mesh infrastructure

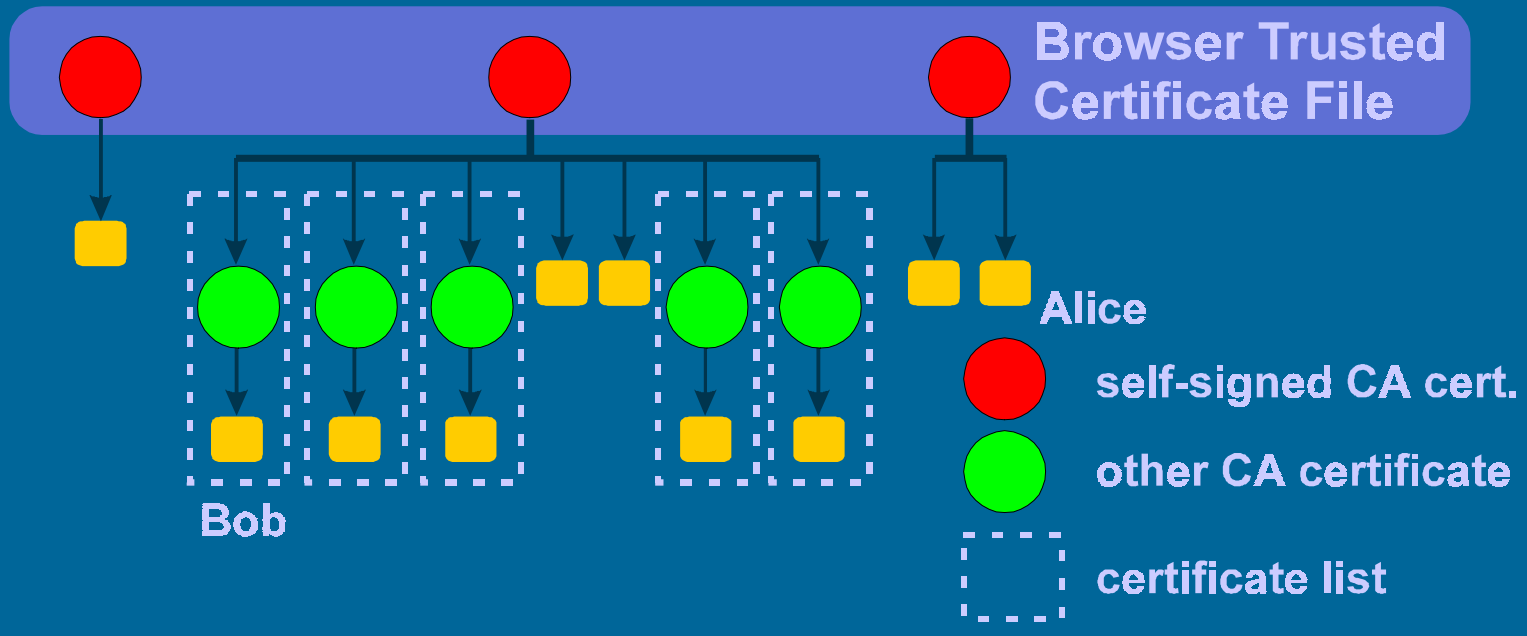
certificate (points issuer to subject)

cross-certificate

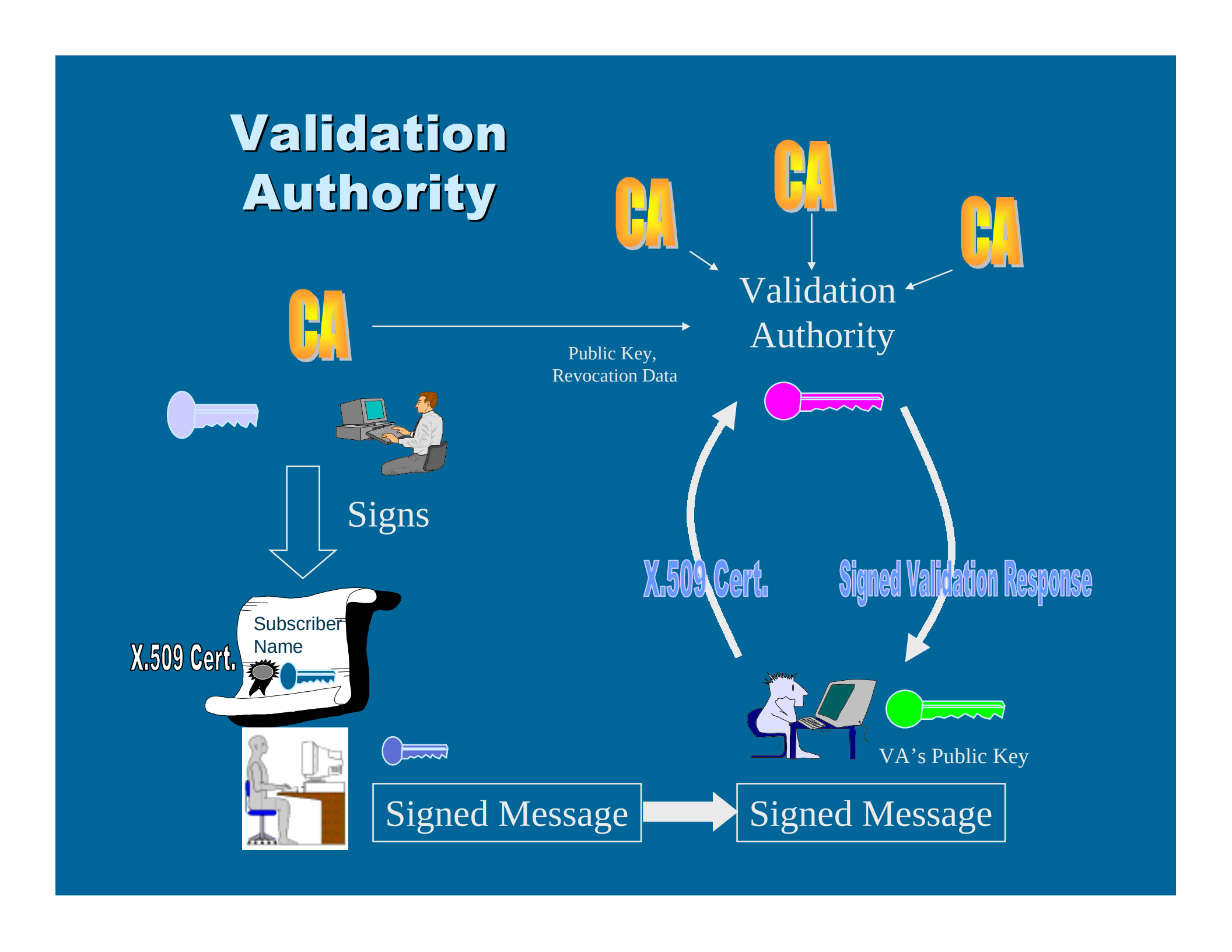
Certification Authority (CA)

user certificate

Trust List


Browser Trusted
Certificate File
Alice
Bob
self-signed CA cert.
other CA certificate
certificate list

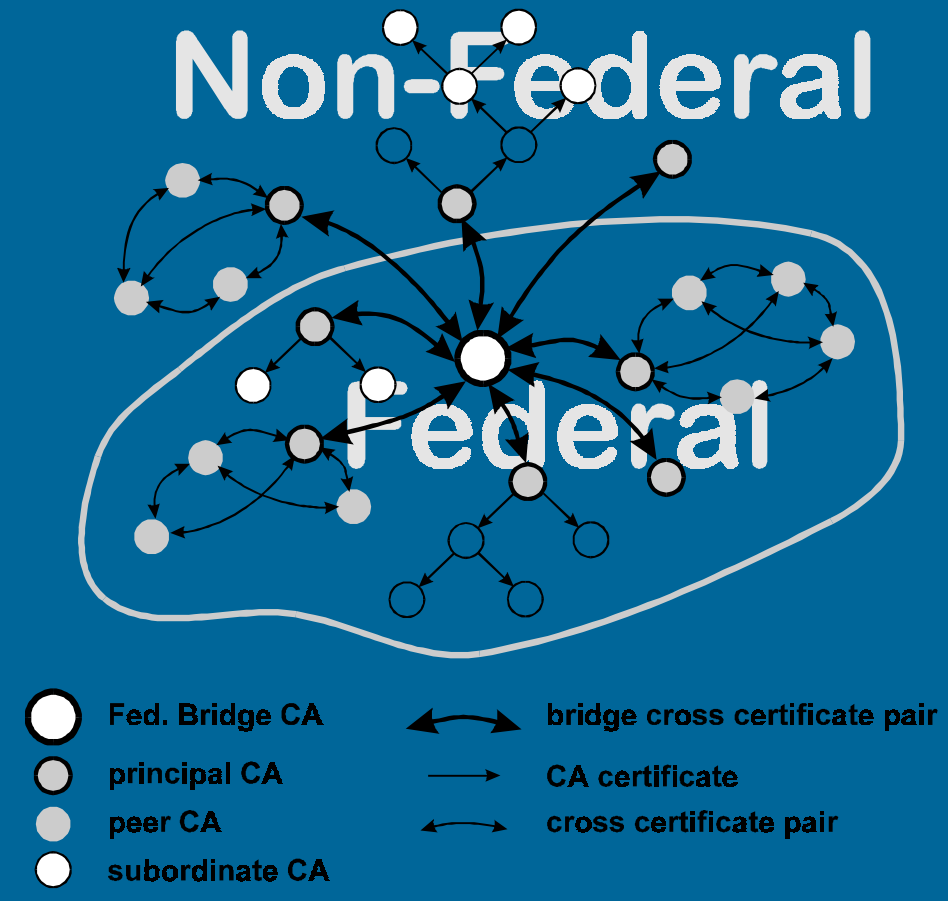
Validation Authority



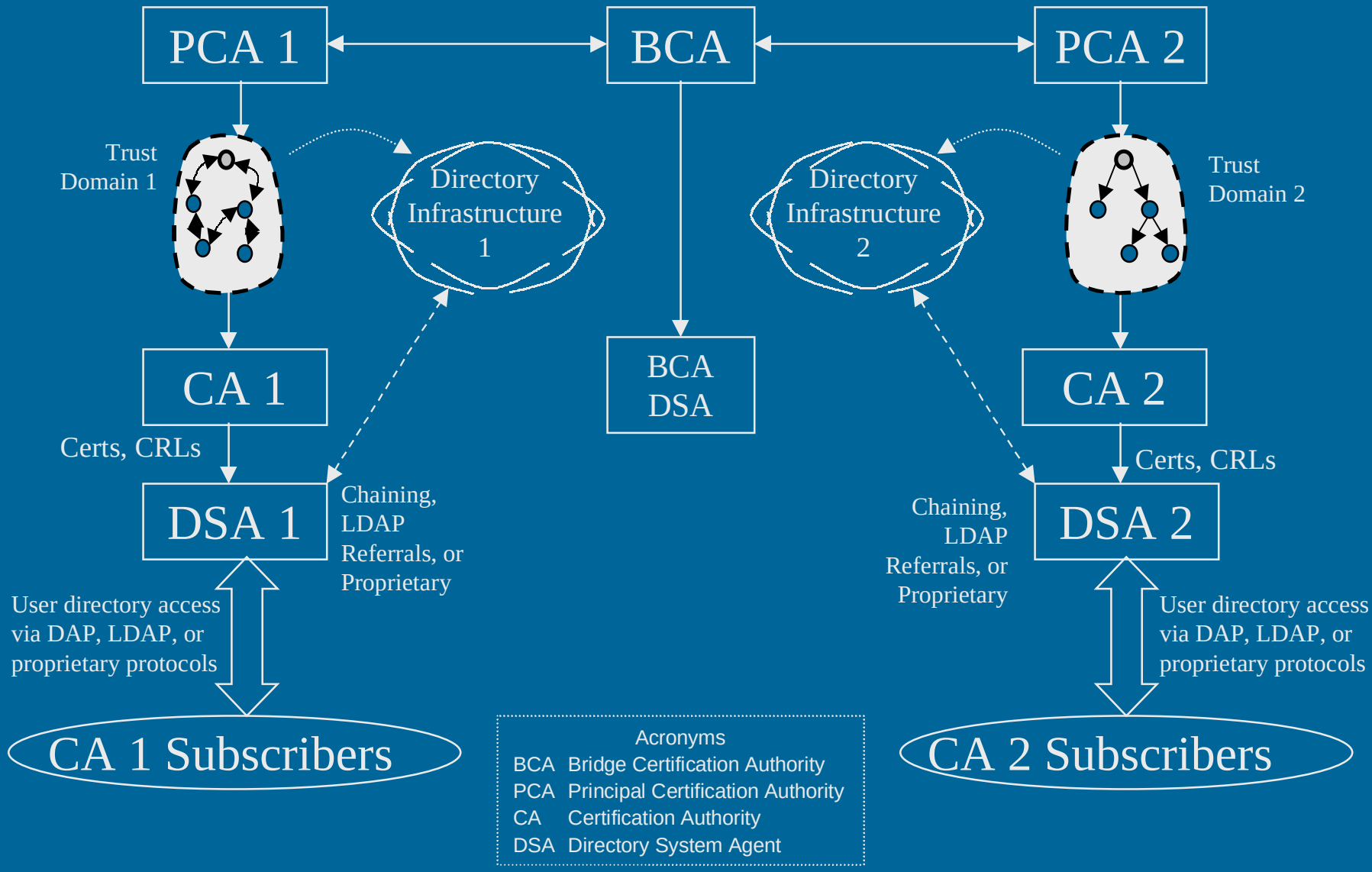
FPKI Proposal

- Build the nexus to connect the pieces
- Three key elements:
  - Federal Policy Management Authority (PMA)
  - Federal “Bridge” CA (BCA)
    - **not a root!**
    - cross certifies with CAs
  - Bridge CA Repository
    - for CA certificates and status

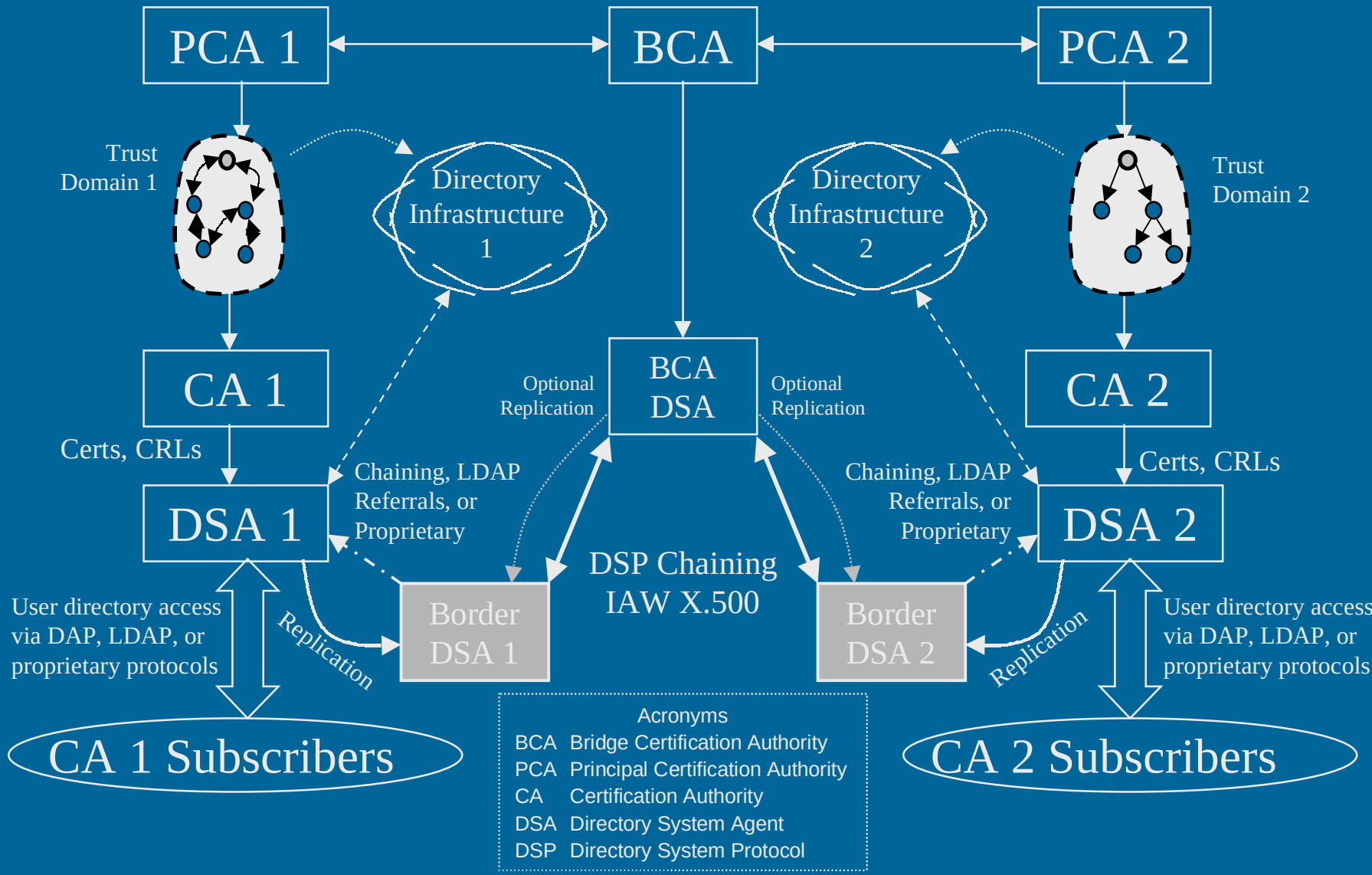
Proposed FPKI Architecture



The BCA Creates Certificate Chains



Chained Border Directories Link the Infrastructures



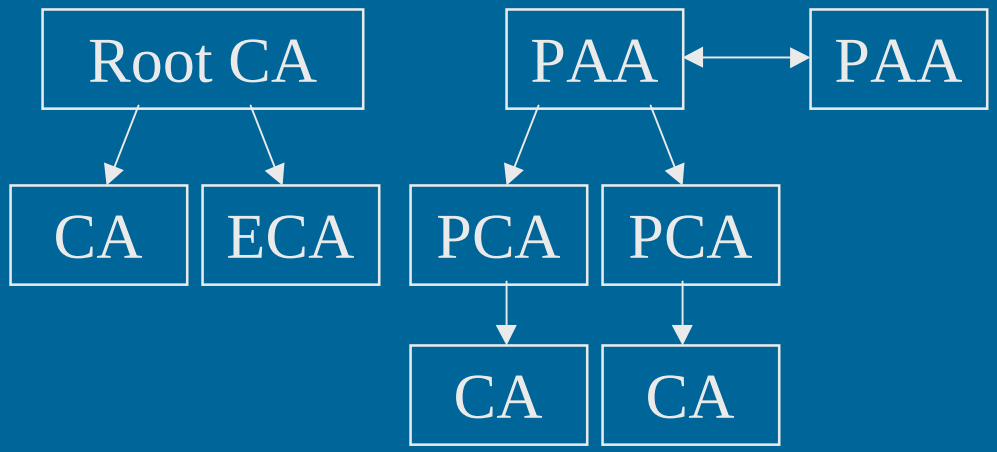
The BCA Demo - Problem Overview

- Three Federal PKIs in which NSA has an investment
  - DoD Class 3 PKI
  - FORTEZZA PKI
  - Federal Bridge Certification Authority PKI
- DoD public key applications will not work outside their own PKI
- Many commercial client products have limitations which make using the BCA difficult

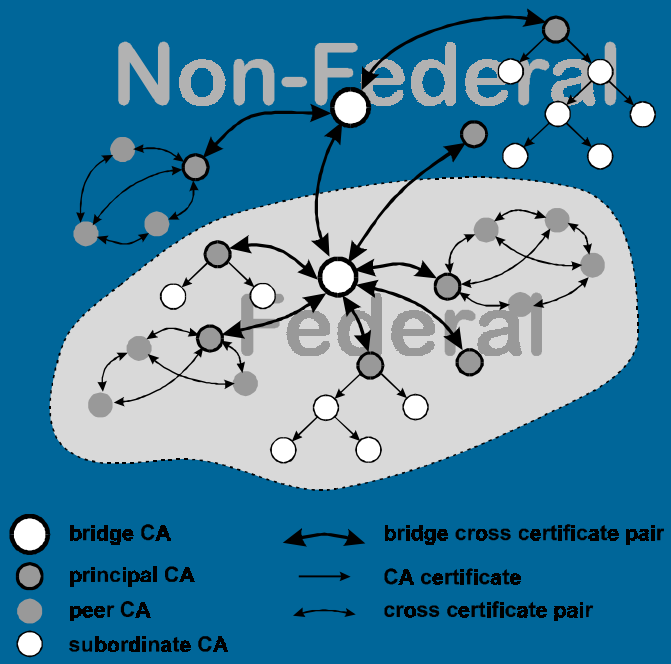
Reasons for PKI Client non-Interoperation

- Certificate chain building
- Cryptographic algorithms
  - RSA vs. KEA and DSS
- Security protocols
  - ACP-120 vs. S/MIME
- Certificate path processing
  - Particularly policy handling
- Directories
  - Schema, access control, protocol profiles
- Access Control

Certificate Chains



DoD Medium



DoD High

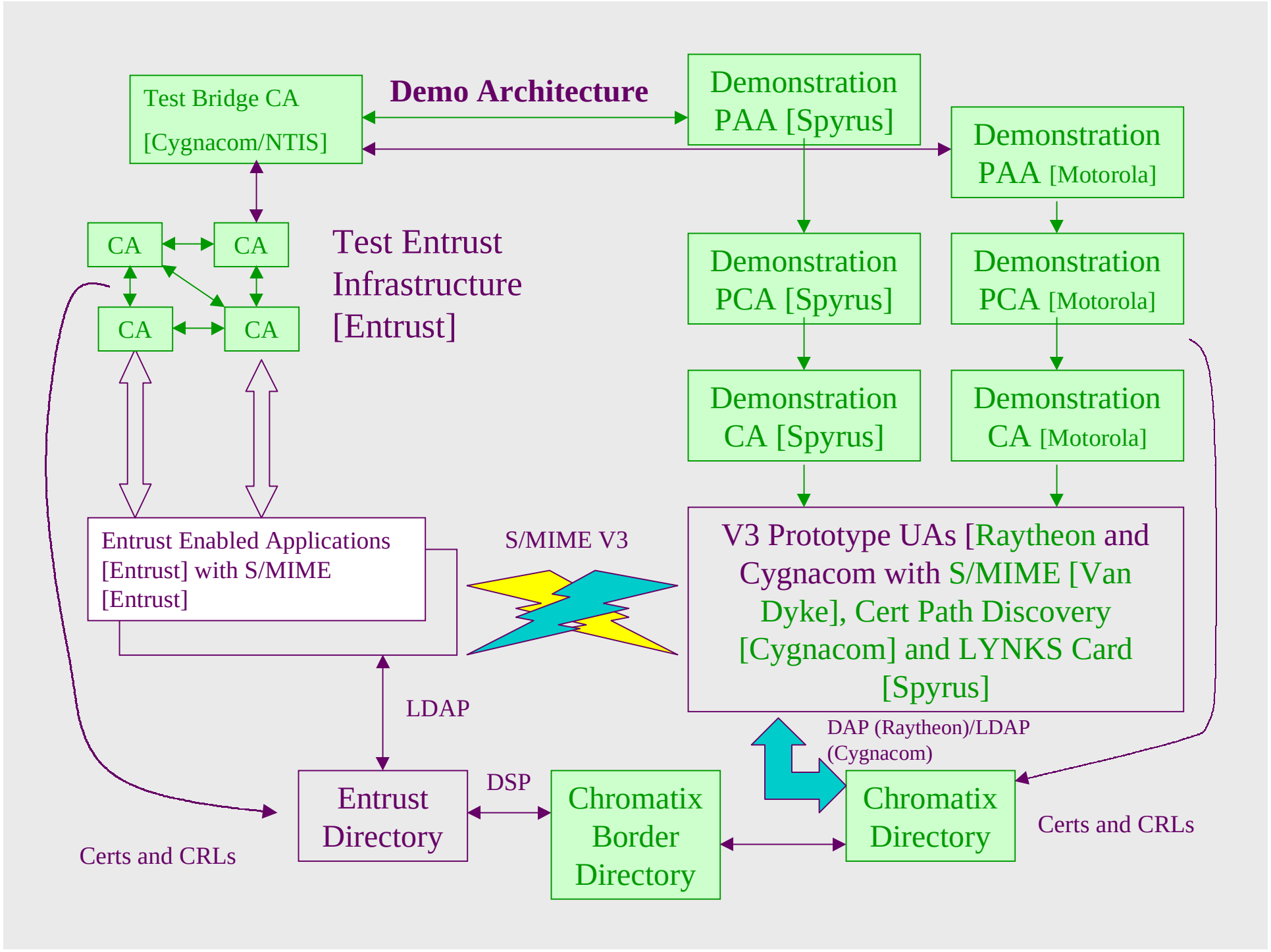
Federal BCA

Proposed Solution Overview

- Development of a Technical Interoperability Profile
  - Minimize deviation from existing commercial standards and practices
  - Minimize impacts to existing applications and infrastructure components
  - Provide a practical migration path from the FORTEZZA based applications to the Interoperability Profile
- Demonstrate the Profile with a Prototype Effort
  - Joint NSA and Entrust

Software Modules

- Certificate Path Development Library
  - Developed by Cygnacom
- Certificate Management Library
  - Developed by J.G. Van Dyke and Associates
- S/MIME Freeware Library
  - Developed by J.G. Van Dyke and Associates


Demo Architecture
Test Bridge CA
[Cygnacom/NTIS]
Demonstration
PAA [Spyrus]
Demonstration
PAA [Motorola]
CA
CA
CA
CA
Test Entrust
Infrastructure
[Entrust]
Demonstration
PCA [Spyrus]
Demonstration
PCA [Motorola]
Demonstration
CA [Spyrus]
Demonstration
CA [Motorola]
Entrust Enabled Applications
[Entrust] with S/MIME
[Entrust]
S/MIME V3
V3 Prototype UAs [Raytheon and
Cygnacom with S/MIME [Van
Dyke], Cert Path Discovery
[Cygnacom] and LYNKS Card
[Spyrus]
LDAP
DAP (Raytheon)/LDAP
(Cygnacom)
Entrust
Directory
DSP
Chromatix
Border
Directory
Chromatix
Directory
Certs and CRLs
Certs and CRLs

What are we getting?

- Promote cross-Federal security interoperation
- Demonstrates a model for allied interoperation
- Provide an option besides trust lists
- Complete interoperability solution, minus labeling and access control
- S/MIME, Cert Path Development and Cert Path Validation SW available for integration into commercial products

Summary

- Bridge CA seems a good approach to achieve interoperability among “equal” public key infrastructures
- Border Directory concept provides “certificate path” interoperability
- Application limitations are a problem
- Bridge CA demonstration attempts to prove technology, and accelerate application developments
- BCA demonstration Phase I planned for completion by 1 October 1999
- Possibility of a Phase II demonstration to demonstrate key recovery, encryption, attribute certificates, multiple signature algorithms.